

Legislative Audit Division

State of Montana



Report to the Legislature

November 1999

Information System Audit

Information Processing Facility and Central Applications

This report provides information regarding general controls over the state computer facility, and application controls over the central computer applications. It contains recommendations to the department for improving controls over the state's central information system environment, including control weaknesses within the Statewide Accounting, Budgeting, and Human Resource System (SABHRS). These recommendations include:

- ▶ Inaccurate calculation of wage garnishments.
- ▶ Errors in conversion data.
- ▶ SABHRS security concerns.

STATE DOCUMENTS COLLECTION

FEB 08 2000

Direct comments/inquiries to:
Legislative Audit Division
Room 135, State Capitol
PO Box 201705
Helena MT 59620-1705

MONTANA STATE LIBRARY
1515 E. 6th AVE.
HELENA, MONTANA 59620

99DP-02

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

PLEASE RETURN



INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and finance.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Linda Nelson, Vice Chair
Senator Reiny Jabs
Senator Ken Miller
Senator Barry "Spook" Stang
Senator Mike Taylor
Senator Jon Tester

Representative Bruce Simon, Chair
Representative Beverly Barnhart
Representative Mary Anne Guggenheim
Representative Dick Haines
Representative Robert Pavlovich
Representative Steve Vick

Legislative Audit Division

Information System Audit

Information Processing Facility and Central Applications

Members of the audit staff involved in this audit were Ken Erdahl, Wendy Kittleson, Rene Silverthorne, and Lon Whitaker.

Table of Contents

	Appointed and Administrative Officials	Page ii
	Report Summary	Page S-1
Chapter I - Introduction and Background	Introduction	Page 1
	Central Payroll/HRMS	Page 2
	SBAS/PeopleSoft Financials	Page 3
	Audit Objectives	Page 4
	Audit Scope and Methodology	Page 4
	Compliance	Page 5
	Summary	Page 5
Chapter II - Data Integrity/Inefficiencies	Introduction	Page 7
	Warrants Issued for \$0.00	Page 7
	Garnishments Not Processed Correctly - Need to be Done Manually	Page 8
	Conversion from PPP to HRMS	Page 9
	Conversion Testing Documentation	Page 10
Chapter III - Security	Introduction	Page 13
	Access not Restricted to Authorized Areas in HRMS	Page 13
	Update and Approval Access Should be Restricted Within PeopleSoft Financials	Page 14
	Access to Correction Mode Should be Removed	Page 16
	Universal Access Should be Restricted	Page 17
	Access to Chartfields Should be Restricted	Page 18
	Minimum Password Parameters Should be Enforced	Page 18
	Disaster Recovery	Page 20
Agency Response	Department of Administration	Page A-2

Appointed and Administrative Officials

Department of Administration

Lois Menzies, Director

Cathy Muri, Administrator
Accounting and Management Support Division

Tony Herbert, Administrator
Information Services Division

Jeff Brandt, Bureau Chief
Policy, Development, and Customer Relations Bureau

Paul Rylander, Bureau Chief
Computer Operations Bureau

John McEwen, Administrator
Personnel Division

Marjorie Rowley, Manager
State Payroll

Brian McCullough, Bureau Chief
SABHRS Support Bureau

Report Summary

Introduction

We conduct a review of central computer applications each year at the Department of Administration (department). We reviewed general controls over the Information Processing Facility (computer center), and application controls over the State Payroll, Warrant Writer, Statewide Budgeting and Accounting System, and the newly implemented Statewide Accounting, Budgeting, and Human Resource System (SABHRS).

A discussion of the audit scope and objectives is included in Chapter I. Further discussion of the audit issues summarized below is included in Chapters II and III. *Overall, we concluded controls over the legacy systems were adequate, but application controls do not provide for controlled application processing for SABHRS.*

Data Integrity/Inefficiencies

At the time of implementation, the information from the legacy systems was transferred, or converted, to SABHRS. In order to ensure the information converted completely and correctly, we performed tests on critical fields, comparing the ending balances from the legacy systems to the beginning balances on SABHRS. We also reviewed various processes and identified areas where SABHRS creates inaccuracies and inefficiencies in processing.

Warrants Issued for \$0.00

Some intermittent or seasonal state employees become "inactive" on the state payroll system, but are still receiving the state insurance benefit. Although they receive no salary, the employer portion of the insurance benefit still needs to be recorded. In order to do this, these employees must be placed in active status, with \$0.00 pay. The system requires anyone in active status who is receiving benefits be issued a warrant each pay period. Consequently, approximately 200 warrants are generated each pay period for \$0.00.

Printing \$0.00 warrants, and employee time to locate, pull and destroy the warrants, is an inefficient use of state resources. The department should either create an edit on the system that suppresses the printing of any warrant for \$0.00, or enhance SABHRS with the capability of processing benefits for inactive employees.

Report Summary

Garnishments not Processed Correctly - Need to be Done Manually

When employees of the state have unpaid debts, often the courts will order a portion of their wages to be withheld, or "garnisheed," and the withheld amount paid to the debtor. The ability to garnishee wages was included as part of the requirement in the contract for development of HRMS. When state Central Payroll receives a request for a garnishment, they enter the amount onto the system, and the system should automatically calculate the amount to be withheld from each paycheck.

In many cases HRMS is not calculating the garnishments correctly, based on Federal and State laws. As a result, if too much is withheld, the state is not in compliance with state and federal law. If too little is withheld, the state is not complying with the court order. Since the inception of HRMS, up to one full-time staff person in Central Payroll has been verifying the calculation of all garnishments manually to ensure they are calculated correctly.

The department should ensure HRMS accurately calculates garnishments in accordance with federal and state law.

Conversion from PPP to HRMS

In order to determine if HRMS began operations with complete information, we compared the personal information and the employee and employer balances from PPP with the beginning information on HRMS.

Using criteria provided by SABHRS personnel, we identified five fields that did not convert. Year-to-date totals for state unemployment, workers' compensation, and public employees' retirement contribution totals have accumulated on SABHRS from the conversion date forward, but FICA and Medicare totals could not be found at all on SABHRS. SABHRS personnel could not provide documentation of why the fields did not convert.

Incomplete year-to-date totals could result in inaccurate reporting. For instance, year-to-date employer totals for public employee retirement contributions are inaccurately reported on employee pay advices. Personnel should ensure all intended data converted completely from the PPP system to the HRMS system.

Conversion Testing Documentation

Prior to conversion from PPP to HRMS, extensive testing was performed to ensure the conversion would be accurate and complete. Various combinations and scenarios were tested in an attempt to identify and correct errors in the system before putting it into production. There were six "mock conversions" for HRMS, where actual data was converted and reviewed in a test database. As errors were identified, programming was done to correct the errors, and the corrections were then tested in the next mock conversion.

We requested documentation of the conversion testing to determine if the testing was comprehensive, and whether the identified errors were resolved prior to implementation. SABHRS personnel could not locate the testing documentation. Documentation of testing and error resolution could be useful in resolving future problems which may be of a similar nature.

Testing was an important part of the overall development process, and documentation of that testing could be a valuable resource in the on-going operation and maintenance of the system. SABHRS personnel should locate and retain any available testing documentation, and ensure all future testing is well documented and retained for their reference.

Security

Access controls provide electronic safeguards designed to protect computer system resources. Logon IDs and passwords control access to the SABHRS operating system, computer programs, and data. Proper access controls prevent and detect deliberate or accidental errors caused by improper use or manipulation of data, programs, and/or computer resources. Limited access based on job duties prevents users from inadvertently or willfully executing programs or changing data unrelated to their job.

We reviewed security access established through SABHRS and identified areas where the department should improve access controls.

Report Summary

Access not Restricted to Authorized Areas in HRMS

During the audit we determined that automated controls do not restrict certain payroll actions to only the payroll information of a specific agency. Agency personnel with security access to enter, change, or approve employee time within their agency can also perform the same functions for any employee in the state. For instance, payroll officers are authorized to enter time for employees within their agency, yet the ability exists to enter time for any employee in any other agency.

We identified examples where human resource officers accidentally changed employees' time at other agencies, causing incorrect warrants to be issued. Access to payroll data should be limited to those individuals authorized to process or maintain specific payroll information. Failure to restrict that access increases the risk that unauthorized changes will be made to the data on the system.

Update and Approval Access Should be Restricted within PeopleSoft Financials

When accounting transactions are made between agencies, rather than writing a warrant from one agency to another, an "inter-unit transaction" is performed. With an inter-unit transaction, one of the agencies originates the transaction and the receiving agency completes and approves the transaction. In order to do this, those individuals involved must have approval access to the other agency's inter-unit transactions. When they are given access to another agency's general ledger, for the purpose of approving inter-unit transactions, that access extends to all transaction types for that agency. For example, if accounting clerks can enter or approve transactions at their agency, and are given access to another agency to approve inter-unit transactions, they will also have the ability to enter or approve all transactions at the other agency--not just the inter-unit transactions.

SABHRS personnel indicated the PeopleSoft software does not allow them to specify access to particular transaction types. Therefore, in order to process inter-unit transactions, access must also be given to all other transactions. Subsequent versions of PeopleSoft Financials may give security personnel the ability to further restrict access. The department should ensure that additional security is included in system upgrades. Meanwhile, the department should investigate available options for controlling access on the current version.

Access to Correction Mode Should be Removed

Within SABHRS panels, different access modes can be granted. "Display Only" allows the user to view information, but does not allow any changes. "Update" allows the user to make changes to the records, but retains a copy of the previous record. "Correction" allows a user to add, change, or delete historical, current, and future data, by overwriting information and leaving no audit trail.

We identified 336 employees with correction mode to various areas on the HRMS system, and 581 employees with correction mode to financial data. Without the accountability that is created by an audit trail, there is increased risk that users could make inappropriate changes to payroll or financial data without detection.

Controls should be in place to prevent, detect and help investigate errors and unusual situations. Correction access should be removed, or closely monitored, to ensure only authorized changes are made to SABHRS data.

Universal Access Should be Restricted

During development of SABHRS, individuals involved in the development were given universal (ALLPNLS) access to perform update and testing functions on the HRMS database. This access gives the user unrestricted, unlogged access to all screens on the system. Given this access level, the individual can make changes to agency files without agency approval, and with no accountability for the integrity of the data.

Now that the system is in production, ALLPNLS access should be restricted or eliminated. We identified 17 individuals with ALLPNLS access to the HRMS database. Of those, six no longer have direct involvement in SABHRS. The remaining 11 users are directly involved in the on-going SABHRS support work. However, since the system is in production, any changes or updates should be made and tested in the test environment and incorporated into production after management approval. SABHRS security personnel should review access granted through the ALLPNLS group, and restrict that access for individuals on the production database.

Report Summary

Access to Chartfields Should be Restricted

In SABHRS, "chartfields" define each field of data on the system. These data fields are used on transactions to reference an accounting distribution. Chartfields include such fields as the agency, department, fiscal year, expenditure type, and revenue type. Chartfields are the backbone of the SABHRS financial structure, and therefore additions and changes to them should be well controlled.

In our review of the SABHRS applications we identified 27 individuals with inappropriate access to change various chartfields. Access to the chartfields should be limited to those individuals directly responsible for their maintenance.

Minimum Password Parameters Should be Enforced

A logon ID, unique to a specific computer user and protected by a password known only to that user, provides a good means of limiting access to appropriate users and helps provide accountability for work performed. We determined SABHRS logon ID and password security is not in compliance with state policy.

Consultants stated PeopleSoft does not intend to enhance its password security management. Rather, reliance on third-party software is an alternative. Additional software could be attached to the system which would allow the department to set and enforce those policies, but SABHRS management have decided the benefits are not worth the cost of the software.

Currently, the department has no way of ensuring state password security policies are being adhered to. Consideration of a third-party password management tool could provide those safeguards.

Disaster Recovery

The department does not have formal disaster recovery procedures over the SABHRS computer applications, to return computing services to normal operations following a disaster. An effective disaster recovery plan should allow management to restore computing operations in a reasonable time to minimize losses.

State policy outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing information and resource requirements necessary to maintain applications; and determining alternate

Report Summary

procedures which may be necessary if recovery cannot be completed in a timely manner.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a formal disaster recovery plan, the department may be unable to process accounting transactions, or pay vendors or employees.

Chapter I - Introduction and Background

Introduction

We conduct a review of central computer applications each year at the Department of Administration (department). We review general controls over the Information Processing Facility (computer center), and application controls over the State Payroll, Warrant Writer, and Statewide Budgeting and Accounting System (SBAS) systems (legacy systems), including Property Accountability and Management System (PAMS). In September 1997, the state of Montana awarded a contract to begin work on the Montana Project to Re-engineer the Revenue and Information Management Environment (MTPRRIME). The project was designed to replace the state's central systems--SBAS, Warrant Writer, PPP, and PAMS--with a commercial integrated software package designed to reshape how the state conducts its accounting, budgeting, human resource management, and procurement. During fiscal year 1998-99, both the legacy systems and SABHRS were used to record transactions. Therefore, we performed audit procedures on both systems.

MTPRRIME implementation was a cooperative effort of the software vendor, PeopleSoft; the contract programmers, Anderson Consulting; and state employees. Although much of the MTPRRIME system was developed from previously created programming, enhancements were added to customize the system to meet the specific needs of the state of Montana.

Montana is the first state in the union to implement the finance, procurement/asset management and human resource systems as a complete package. Upon system implementation on July 1, 1999, MTPRRIME was renamed the Statewide Accounting, Budgeting, and Human Resource System (SABHRS). For the remainder of this document, the system will be referred to as SABHRS.

The SABHRS mission statement is: **To create a statewide information system to more effectively manage state resources and serve the citizens of Montana.**

Chapter I - Introduction and Background

Central Payroll/HRMS

Through April 1999, the Department of Administration, State Personnel Division, was responsible for operating the **Payroll/Personnel/Position Control (PPP)** application. Effective on the pay period ending April 23, 1999, PPP was replaced by the PeopleSoft **Human Resource Management System (HRMS)**. HRMS consists of four modules:

Time and Labor:	Bi-Weekly time is input to the Time and Labor module, and “rules” are applied, defining such things as how overtime is paid (compensatory time, time and one-half, straight time, etc.), established work week, etc.
Human Resource:	The Human Resource module tracks information on the individual employees (name, address, emergency contacts, etc.), and on the jobs within each agency (salary, grade, position requirements, location, etc.).
Benefits Administration:	The Benefits Administration module tracks and distributes benefits, such as vacation time, sick leave, medical and life insurance, etc., for each employee.
Payroll:	The Payroll module pulls information from the other three modules, and calculates and prints the paychecks for the pay period.

With the implementation of HRMS, much of the control over the system and the data contained therein became less centralized, with the agencies having the ability to enter and approve payroll and personnel information directly to the system.

Chapter I - Introduction and Background

SBAS/PeopleSoft Financials

The **Statewide Budgeting and Accounting System (SBAS)** was the state's centralized budgeting and accounting system. PeopleSoft's **Financial** system replaced SBAS July 1, 1999. Fiscal year 1998-99 transactions were processed on SBAS through fiscal year-end 1999, and all fiscal year 1999-2000 and subsequent transactions are now processed on the PeopleSoft Financials. PeopleSoft Financials are made up of five modules:

1. Accounts Receivable (A/R)
2. Accounts Payable (A/P)
3. General Ledger (G/L)
4. Asset Management (AM)
5. Purchasing

The **Accounts Receivable (A/R)** module provides many ways to process A/R information. This module calculates and stores client history, determines aging schedules, performs trend analysis, applies payments to customers, etc. The nature of business within numerous agencies does not require the features of the A/R module. Those agencies process their receivables directly to the G/L.

The **Accounts Payable (A/P)** module manages cash disbursements to optimize cash flow. This module can establish payment terms, collect vendor statistics and allow identification of 1099 vendors. A/P integrates with G/L, AM and Purchasing. Agencies use their discretion as to whether their business needs require the A/P functionality or whether direct entry to G/L is most appropriate.

The agencies that use the A/R and A/P modules input their transactions directly to those modules, and the general ledger is updated from those modules through a nightly batch process. Other agencies enter their transactions directly into the General Ledger.

The **Asset Management (AM)** module replaced the **Property Asset Management System (PAMS)** which accounts for state property inventory. PAMS was taken off-line July 1998, and AM was implemented September 1, 1998. In the interim, manual records were maintained by agencies and entered to AM after September 1.

Chapter I - Introduction and Background

Not all agencies converted to AM. Some agencies track assets using their own internal systems. Participation in AM is not mandatory. For those agencies using AM, many only input assets valued over \$5000, but some agencies have opted to include assets valued under \$5000, for tracking purposes.

Due to the time and/or resource restrictions within their agencies, thirteen processing functions within five agencies were not able to meet the implementation schedule for PeopleSoft Financials. A contingency plan was implemented in the form of a "translate" process. Financial transactions are processed and updated using the SBAS programming, coding the transactions in SBAS format. The translate process converts the SBAS data to PeopleSoft format, and then uploads the converted information to the PeopleSoft Financials system. Full conversion of those agencies is expected to take place within the next two years.

Audit Objectives

The objectives of this annual audit included identifying and testing central controls over state data processing applications. For fiscal year 1998-99, both the legacy systems and the SABHRS were in production. We reviewed SBAS, Central Payroll, and Warrant Writer to ensure controls were in place and the applications processed as intended. We also reviewed SABHRS HRMS and Financials, to identify controls in place over those applications.

Audit Scope and Methodology

The audit was conducted in accordance with governmental auditing standards published by the United States General Accounting Office. We evaluated controls over input, processing and output, as well as physical and electronic security.

Because of the significant changes due to the implementation of SABHRS, we gathered information to gain assurances over both the legacy systems and the new systems for the audit period, fiscal year 1998-99.

The SABHRS Asset Management module was implemented September 1998, and the HRMS application was placed into production in April 1999. The SABHRS Financials application,

Chapter I - Introduction and Background

which replaced SBAS and Warrant Writer, was put into production on July 1, 1999. We identified controls in place over both legacy and the SABHRS applications, including electronic and physical security and input, processing and output controls. Since SABHRS was in production for only a portion of the audit period, we did not perform in-depth testing of controls that are in place over SABHRS Financials. However, we identified serious control weaknesses which could have a significant impact on the overall integrity and security of the systems. We also reviewed the accuracy of data conversion from the legacy systems to SABHRS, and whether interfaces between systems are reliable.

Compliance

We reviewed compliance with certain state laws and administrative rules which relate to the central computer applications. Except as noted on pages 18 to 20, we found the department to be in compliance with applicable laws and state policy.

Summary

In conclusion, we found controls provided for controlled application processing on the legacy systems. However, we found weaknesses in electronic security over SABHRS. We also noted weaknesses which compromise data integrity and reduce the effectiveness and efficiency of the SABHRS applications.

Chapter II - Data Integrity/Inefficiencies

Introduction

At the time of implementation, the information from the legacy systems was transferred, or converted, to the new systems. In order to ensure the information converted completely and correctly, we performed tests on critical fields, comparing the ending balances from the legacy systems to the beginning balances on the new systems. We also reviewed various processes and identified areas where SABHRS creates inaccuracies and inefficiencies in processing. These issues are discussed in the following sections.

Warrants Issued for \$0.00

Some intermittent or seasonal state employees become "inactive" on the state payroll system, but are still receiving the state insurance benefit. Although they receive no salary, the employer portion of the insurance benefit still needs to be recorded. During the audit we determined when employees are listed as inactive on HRMS, the system will not record a benefit. As a result, these employees are placed in active status, with \$0.00 pay. The system requires anyone in active status who is receiving benefits be issued a warrant each pay period. Consequently, approximately 200 warrants are generated each pay period for \$0.00. A report is generated by Central Payroll to identify the \$0.00 warrants. Central Payroll personnel then manually locate the warrants and remove them prior to distribution. The \$0.00 warrants are then stored for shredding at a later date.

Printing \$0.00 warrants, and employee time to locate, pull and destroy the warrants, is an inefficient use of state resources. The department should either create an edit on the system that suppresses the printing of any warrant for \$0.00, or enhance SABHRS with the capability of processing benefits for inactive employees.

Recommendation #1

We recommend the department:

- A. Review the feasibility of creating an edit on the system that will suppress the printing of \$0.00 warrants, or
- B. Program the system so benefits can be recorded for inactive employees.

Chapter II - Data Integrity/Inefficiencies

Garnishments Not Processed Correctly - Need to be Done Manually

When employees of the state have unpaid debts, often the courts will order a portion of their wages to be withheld, or “garnisheed,” and the withheld amount paid to the debtor. The ability to garnishee wages was included as part of the requirement in the contract for development of HRMS. When state Central Payroll receives a request for a garnishment, they enter the amount onto the system, and the system should automatically calculate the amount to be withheld from each paycheck.

Federal and state law defines the maximum percentage of wages which can be withheld from employees for garnishments, based on their pay and filing status. In determining the amount to apply the percentage to, certain benefits are included and certain deductions are excluded from gross wages prior to applying the percent. In many cases, HRMS is not calculating the garnishments correctly. For example, the employer share of health benefits is not included correctly when determining the total that can be garnisheed from a paycheck. As a result, if too much is withheld, the state is not in compliance with state and federal law. If too little is withheld, the state is not complying with the court order. Since the inception of HRMS, Central Payroll has been verifying the calculation of all garnishments manually to ensure they are calculated correctly, and if there is a difference they override the system calculations and enter the correct figures.

SABHRS personnel stated they are aware of the problem, and will ensure subsequent versions of the software are updated to resolve the issue. At the time of our audit, a Central Payroll employee indicated the re-calculation and re-entry of garnishments required the full time of one staff person.

The department should ensure HRMS accurately calculates garnishments in accordance with federal and state law.

Chapter II - Data Integrity/Inefficiencies

Recommendation #2

We recommend the department:

- A. Ensure garnishments are calculated correctly by HRMS, and
- B. Ensure subsequent HRMS versions process garnishments correctly.

Conversion from PPP to HRMS

In order to determine if HRMS began operations with complete information, we compared the personal information and the employee and employer balances from PPP with the beginning information on HRMS.

Using criteria provided by SABHRS personnel, we selected a sample of fields intended for conversion, and identified the following fields that did not convert:

- ▶ Employer share of state unemployment insurance
- ▶ Employer share of workers' compensation insurance
- ▶ Employer share of public employees' retirement contributions
- ▶ Employer share of FICA
- ▶ Employer share of Medicare

The state unemployment, workers' compensation, and public employees' retirement contribution totals are on SABHRS from the conversion date forward, but FICA and Medicare totals no longer exist on SABHRS. SABHRS personnel could not provide documentation of why the fields did not convert.

Incomplete year-to-date totals could result in inaccurate reporting. For instance, year-to-date employer totals for public employee

Chapter II - Data Integrity/Inefficiencies

retirement contributions are inaccurately reported on employee pay advices.

SABHRS personnel indicated that conversion testing was performed; however, personnel could provide no documentation of test results. Personnel should ensure all intended data converted completely from the PPP system to the HRMS system.

Recommendation #3

We recommend the department identify all differences between PPP and HRMS, and ensure intended data converted completely and accurately.

Conversion Testing Documentation

Prior to conversion from PPP to HRMS, extensive testing was performed to ensure the conversion would be accurate and complete. Various combinations and scenarios were tested in an attempt to identify and correct errors in the system before putting it into production. There were six “mock conversions” for HRMS, where actual data was converted and reviewed in a test database. As errors were identified, programming was done to correct the errors, and the corrections were then tested in the next mock conversion.

We requested documentation of the conversion testing to determine if the testing was comprehensive, and whether the identified errors were resolved prior to implementation. SABHRS personnel indicated there was documentation of the testing, but were unable to locate it. They were unsure whether the documentation was destroyed, or if it was retained by personnel from the consulting firm that helped develop the system.

As errors are identified on the system, department personnel should determine whether similar problems were already addressed during testing, and how the problems were resolved. Thus, in many cases, the resolution of the errors may be expedited. System upgrades can be expected approximately every 18 months. With the upgrades, similar problems may arise which have already been identified on the old version where solutions have been developed and tested.

Chapter II - Data Integrity/Inefficiencies

Many of the original developers of the system are no longer available to help support the on-going maintenance of the system. The personnel from the consulting firm are no longer in Montana, and many of the state employees involved in the development have returned to their prior jobs, or have taken jobs outside of state government. Therefore, much of the work done in testing could only be recalled through documentation.

Testing was an important part of the overall development process, and documentation of that testing could be a valuable resource in the on-going operation and maintenance of the system. SABHRS personnel should locate and retain any available testing documentation, and ensure all future testing is well documented and retained for their reference.

Recommendation #4

We recommend the department:

- A. Obtain the documentation of conversion testing performed on the system, and**
- B. Ensure all future testing is documented and the documentation retained by the state.**

Chapter III - Security

Introduction

Access controls provide electronic safeguards designed to protect computer system resources. Logon IDs and passwords control access to the SABHRS operating system, computer programs, and data. Proper access controls prevent and detect deliberate or accidental errors caused by improper use or manipulation of data, programs, and/or computer resources. Limited access based on job duties prevents users from inadvertently or willfully executing programs or changing data unrelated to their job.

Operator security is a tool used by SABHRS to permit system users to log into the system with specific levels of access. Each user of SABHRS is assigned an operator ID. Operator IDs with similar access needs are assigned to an operator class. Classes are further assigned access to specific menus and panels within the system. SABHRS users can only be assigned to a single operator class.

We reviewed security access established through SABHRS and identified areas where the department should improve access controls. Our findings are discussed in the following sections.

Access not Restricted to Authorized Areas in HRMS

During the audit we determined that automated controls do not restrict certain payroll actions to only the payroll information of a specific agency. Agency personnel with security access to enter, change, or approve employee time within their agency can also perform the same functions for any employee in the state. For instance, payroll officers are authorized to enter time for employees within their agency, yet the ability exists to enter time for any employee in any other agency. Their access restricts them to certain types of transactions, but does not distinguish between departments or agencies.

We identified examples where human resource officers accidentally changed employees' time at other agencies, causing incorrect warrants to be issued. At any time during the input, authorization and correction process, anyone with similar access can change the employee time, and the agency human resource officers would not be aware of the changes. Only through individual review of each

payroll transaction can agencies be assured no inappropriate changes are made.

The PeopleSoft software has the ability to restrict user access to screens and information within particular areas of the system, through operator classes. For instance, a particular employee's access could be restricted so he could only update particular areas within a division or agency. However, SABHRS personnel stated setting up individual access is very time consuming; therefore, they have opted to create statewide access groups of users who do similar tasks.

Access to payroll data should be limited to those individuals authorized to process or maintain specific payroll information. Failure to restrict that access increases the risk that unauthorized changes will be made to the data on the system.

Recommendation #5

We recommend the department:

- A. Establish controls to limit employee access to only those payroll transactions for which the person has authority, or**
- B. Establish compensating controls to identify and monitor changes made to personal payroll records, or to records of employees outside the department.**

Update and Approval Access Should be Restricted Within PeopleSoft Financials

When accounting transactions are made between agencies, rather than writing a warrant from one agency to another, an "inter-unit transaction" is performed. With an inter-unit transaction, one of the agencies originates the transaction and the receiving agency completes and approves the transaction. In order to do this, those individuals involved must have approval access to the other agency's transactions.

Within SABHRS financials, each individual is assigned to an operator class, which specifies what types of things can be accessed,

and at what level. Unlike HRMS, this access can be further restricted so individuals can only access information within their agency or department. However, when they are given access to another agency's general ledger, for the purpose of approving inter-unit transactions, that access extends to all transaction types for that agency. For example, if accounting clerks can enter or approve transactions at their agency, and are given access to another agency to approve inter-unit transactions, they will also have the ability to enter or approve all transactions at the other agency--not just the inter-unit transactions.

In order to reduce the risk of misuse of the system, financial transactions should be entered by one person and approved by another, to prevent any one person from processing inappropriate transactions. The enterer and approver are then both responsible for the content and purpose of the transaction. However, when multiple people have enter or approve ability for an agency's transactions, it is more difficult to establish accountability for changes made on the system.

SABHRS personnel indicated the PeopleSoft software does not allow them to specify access to particular transaction types. Therefore, in order to process inter-unit transactions, access must also be given to all other transactions. Subsequent versions of PeopleSoft Financials may give security personnel the ability to further restrict access. The department should ensure that additional security is included in system upgrades. Meanwhile, the department should investigate available options for controlling access on the current version.

Recommendation #6

We recommend the department:

- A. Implement controls over access by users who perform inter-unit transactions, and**
- B. Ensure new upgrades of the software include additional security features.**

Chapter III - Security

Access to Correction Mode Should be Removed

Within SABHRS panels, different access modes can be granted. "Display Only" allows the user to view information, but does not allow any changes. "Update" allows the user to make changes to the records, but retains a copy of the previous record. "Correction" allows a user to add, change, or delete historical, current, and future data, by overwriting information and leaving no audit trail.

Personnel with correction mode can make changes to certain employee payroll information or financial information, with no accountability for the changes. For instance, a human resource officer could make a change to a pay rate or deductions for an employee using correction mode, and the payroll personnel may not be aware of the change. There is no record of what changes were made, who made them, or when they were made. Similarly, someone with correction mode for the financials vendor table can change the name and address of any vendor, with no trail of the previous values.

We identified 336 employees with correction mode to various areas on the HRMS system, and 581 employees with correction mode to financial data. Without the accountability that is created by an audit trail, there is increased risk that users could make inappropriate changes to payroll or financial data without detection.

Prior to putting the system into production, SABHRS personnel stated they would remove correction access for all but a few select individuals, recognizing the potential risk associated with that type of access. However, once the system was put into production, there were errors in conversion, production, and data entry, and management determined correction mode was necessary for many employees to help correct errors and to help expedite the system processes. However, changes to data on the system could be made in update mode, leaving a historical trail of all changes made to the data.

Controls should be in place to prevent, detect and help investigate errors and unusual situations. Correction access should be removed, or closely monitored, to ensure only authorized changes are made to SABHRS data.

Recommendation #7

We recommend the department remove, or closely monitor, “correction” mode access to SABHRS production data.

Universal Access Should be Restricted

During development of SABHRS, individuals involved in the development were given universal (ALLPNLS) access to perform update and testing functions on the HRMS database. This access gives the user unrestricted, unlogged access to all screens on the system. Given this access level, the individual can make changes to agency files without agency approval, and with no accountability for the integrity of the data.

Now that the system is in production, ALLPNLS access should be restricted or eliminated. We identified 17 individuals with ALLPNLS access to the HRMS database. Of those, three are from the consulting firm involved in the development of SABHRS, and now have little or no involvement with the system. Two are agency personnel who were involved in the project, but are now working full-time at their agencies, and one is involved as a SABHRS trainer. The remaining 11 users are directly involved in the on-going SABHRS support work. SABHRS personnel stated their access is necessary to help users in resolving errors and problems.

Since the system is in production, any changes or updates should be made and tested in the test environment and incorporated into production after management approval. SABHRS security personnel should review access granted through the ALLPNLS group, and restrict that access for individuals on the production database.

Recommendation #8

We recommend the department review access privileges, and restrict access through the ALLPNLS group.

Chapter III - Security

Access to Chartfields Should be Restricted

In SABHRS, "chartfields" define each field of data on the system. These data fields are used on transactions to reference an accounting distribution. Chartfields include such fields as the agency, department, fiscal year, expenditure type, and revenue type. Chartfields are the backbone of the SABHRS financial structure, and therefore additions and changes to them should be well controlled.

In our review of the SABHRS applications we identified 27 individuals with inappropriate access to change various chartfields. SABHRS personnel were not aware of the access until brought to their attention by the audit, and agreed the access should be restricted. Inappropriate changes to the chartfields could result in incorrect accounting of revenue and expenditure transactions. Access to the chartfields should be limited to those individuals directly responsible for their maintenance.

In order to ensure access to chartfields is reasonable, SABHRS security personnel should periodically review chartfield access, and remove access for anyone who does not have maintenance responsibility.

Recommendation #9

We recommend the department:

- A. Periodically review the access allowed to the SABHRS chartfields, and**
- B. Remove access for people not responsible for chartfield maintenance.**

Minimum Password Parameters Should be Enforced

A logon ID, unique to a specific computer user and protected by a password known only to that user, provides a good means of limiting access to appropriate users and helps provide accountability for work performed. We determined SABHRS logon ID and password security could be improved.

The password is the key to a user's system access. The state of Montana established policies for passwords, designed to help protect access to the state's resources. The legacy systems (SBAS, PPP) operated on the mainframe, and were protected by the mainframe security functionality. The SABHRS applications do not operate on the mainframe, and the present software does not have the capability of enforcing minimum password standards. State policy includes:

- a) Passwords must be at least six characters long;
 - cannot set minimum length in SABHRS.
- b) Passwords must contain at least one numeric and one alphabetic character;
 - cannot restrict SABHRS password content to contain letters and numbers.
- c) Passwords must not be obvious or easily guessed (user ID, user's name, address, birth date, child's name, spouse's name);
 - cannot compare and restrict personal password information on SABHRS.
- d) Passwords must be changed at least every 60 days;
 - SABHRS cannot automatically disable accounts when passwords are not changed.
- e) Passwords must not be reused for at least four cycles.
 - SABHRS cannot restrict new passwords based on whether they have been used before.

Consultants stated PeopleSoft does not intend to enhance its password security management. Rather, reliance on third-party software is an alternative. Additional software could be attached to the system which would allow the department to set and enforce those policies, but SABHRS management have decided the benefits are not worth the cost of the software.

Chapter III - Security

Currently, the department has no way of ensuring state password security policies are being adhered to. Consideration of a third-party password management tool could provide those safeguards.

Recommendation #10

We recommend the department develop safeguards to ensure state password security policies are adhered to.

Disaster Recovery

The department does not have formal disaster recovery procedures over the SABHRS computer applications, to return computing services to normal operations following a disaster. An effective disaster recovery plan should allow management to restore computing operations in a reasonable time to minimize losses.

State policy outlines agency responsibilities regarding disaster recovery which include assigning recovery team member responsibilities; assessing information and resource requirements necessary to maintain applications; and determining alternate procedures which may be necessary if recovery cannot be completed in a timely manner.

The state has developed a disaster plan, including an off-site backup facility, for the mainframe operations. However, the SABHRS applications do not operate on the mainframe and are not included in the mainframe plan.

Documented and tested recovery procedures allow normal operations to resume as quickly as possible following a disaster. Without a formal disaster recovery plan, the department may be unable to process accounting transactions, or pay vendors or employees.

Recommendation #11

We recommend the department establish, test, and document a formal disaster recovery plan.

Agency Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE



MARC RACICOT, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032
FAX 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

November 30, 1999

NOV 30 1999

Scott A. Seacat, Legislative Auditor
Legislative Audit Division
State Capitol
Helena, MT 59620

Dear Mr. Seacat:

We have reviewed the recommendations pertaining to the Information Processing Facility and Central Applications Audit for the fiscal year ended June 30, 1999. Our responses follow:

RECOMMENDATION #1: WE RECOMMEND THE DEPARTMENT:

- A. REVIEW THE FEASIBILITY OF CREATING AN EDIT ON THE SYSTEM THAT WILL SUPPRESS THE PRINTING OF \$0.00 WARRANTS, OR
- B. PROGRAM THE SYSTEM SO BENEFITS CAN BE RECORDED FOR INACTIVE EMPLOYEES.

Response: We concur. The system is designed to create a warrant for any employee who has earnings. The employer portion of insurance benefits is an earning. The earning is deducted from the employee to pay for insurance benefits, which results in the \$0.00 warrant. We would like to be able to suppress the printing of these warrants. By April 1, 2000, we will make a determination regarding the feasibility and cost of modifying the software versus the ongoing cost of manually removing the warrants from distribution.

RECOMMENDATION #2: WE RECOMMEND THE DEPARTMENT:

- A. ENSURE GARNISHMENTS ARE CALCULATED BY HRMS, AND
- B. ENSURE SUBSEQUENT HRMS VERSIONS PROCESS GARNISHMENTS CORRECTLY.

Response: We concur. In our ongoing review of the garnishment process, we have made some adjustments in the process and have learned more about the capabilities of the software. Presently, checking calculations and re-entering the correct garnishment amount takes less than a day every two weeks. The new software has improved the process. Garnished employees receive their paycheck at the same time as all other employees, whereas under the old system these employees received their paycheck a day later. The next release of the software should resolve the problems pointed out in the audit.

RECOMMENDATION #3: WE RECOMMEND THE DEPARTMENT IDENTIFY ALL DIFFERENCES BETWEEN PPP AND HRMS, AND ENSURE INTENDED DATA CONVERTED COMPLETELY AND ACCURATELY.

Response: We concur. Department staff is currently reviewing the converted data to insure that accurate W-2s are processed by January 31, 2000.

RECOMMENDATION #4: WE RECOMMEND THE DEPARTMENT:

- A. OBTAIN THE DOCUMENTATION OF CONVERSION TESTING PERFORMED ON THE SYSTEM, AND
- B. ENSURE ALL FUTURE TESTING IS DOCUMENTED AND THE DOCUMENTATION RETAINED BY THE STATE.

Response: We concur. We have obtained the available information on conversion testing. Additionally, we will document future testing and retain this documentation.

RECOMMENDATION #5: WE RECOMMEND THE DEPARTMENT:

- A. ESTABLISH CONTROLS TO LIMIT EMPLOYEE ACCESS TO ONLY THOSE PAYROLL TRANSACTIONS FOR WHICH THE PERSON HAS AUTHORITY, OR

ESTABLISH COMPENSATING CONTROLS TO IDENTIFY AND MONITOR CHANGES MADE TO PERSONAL PAYROLL RECORDS, OR TO RECORDS OF EMPLOYEES OUTSIDE THE DEPARTMENT.

Response: We concur. The Department will work with agencies by reviewing operator classes that are required to meet agency business processes. If compensating controls are determined to be necessary by agencies or the Department, the Department will develop these controls for the central business processes and/or recommend controls that may be used by agencies. We plan to complete these tasks by January 30, 2000.

RECOMMENDATION #6: WE RECOMMEND THE DEPARTMENT:

- A. IMPLEMENT CONTROLS OVER ACCESS BY USERS WHO PERFORM INTER-UNIT TRANSACTIONS, AND
- B. ENSURE NEW UPGRADES OF THE SOFTWARE INCLUDE ADDITIONAL SECURITY FEATURES.

Response: We partially concur. SABHRS Support Bureau staff believe adequate procedural controls are in place for individuals performing inter-unit transactions. This belief is based upon the following considerations: 1) Agency accounting managers were advised that they should carefully consider who is provided with the authority to perform inter-unit transactions. Only a limited number of trained accountants should perform these duties; 2) State policy directs agency staff to review processed transactions to verify validity. Agencies following this policy will identify invalid transactions; 3) The same person cannot enter and approve non-journal transactions, such as vouchers; 4) An audit function records the ID associated with operators entering and approving financial transactions. Once a reporting mechanism is in place, agency staff will have the ability to identify transactions entered or approved by an operator associated with a different agency.

The SABHRS Support Bureau staff will, however, continue to pursue the implementation of all practical approaches that will improve the system's controls over the processing of transactions.

RECOMMENDATION #7: WE RECOMMEND THE DEPARTMENT REMOVE, OR CLOSELY MONITOR, "CORRECTION" MODE ACCESS TO SABHRS PRODUCTION DATA.

Response: We concur. The Department will monitor closely the availability of the "correction" mode that is available in PeopleSoft. The Department will work with agencies to insure that the correction feature is only used as required by the business process.

RECOMMENDATION #8: WE RECOMMEND THE DEPARTMENT REVIEW ACCESS PRIVILEGES AND RESTRICT ACCESS THROUGH THE ALLPNLS GROUP.

Response: We concur. The SABHRS Support Bureau has removed the consultants and agency personnel who are no longer involved in ongoing support of SABHRS from access through the ALLPNLS group.

RECOMMENDATION #9: WE RECOMMEND THE DEPARTMENT:

- A. PERIODICALLY REVIEW THE ACCESS ALLOWED TO THE SABHRS CHARTFIELDS, AND
- B. REMOVE ACCESS FOR PEOPLE NOT RESPONSIBLE FOR CHARTFIELD MAINTENANCE.

Response: We concur. The Department has removed the ability to add various chartfield values from those operators who were inappropriately provided with such authority.

RECOMMENDATION #10: WE RECOMMEND THE DEPARTMENT DEVELOP SAFEGUARDS TO ENSURE STATE PASSWORD SECURITY POLICIES ARE ADHERED TO.

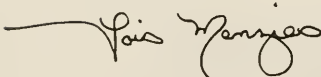
Response: We concur. We will develop appropriate changes to our security policies or system access procedures by June 30, 2000.

RECOMMENDATION #11: WE RECOMMEND THE DEPARTMENT ESTABLISH, TEST AND DOCUMENT A FORMAL DISASTER RECOVERY PLAN.

Response: We concur. We plan to test and document a disaster recovery plan by June 30, 2000.

We appreciate the opportunity to work with your staff on these issues.

Sincerely,

A handwritten signature in black ink, appearing to read "Lois Menzies", with a long horizontal line extending to the left.

LOIS MENZIES
Director

